

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of detecting scanning attacks, comprises:
adding host-pair connection records to a connection table when each time a host accesses another host;
at the end of a first short update period, accessing the connection table to determine new host pairs;
determining the number of new host pairs added to the table over the first short update period; and
if a host has made more than a first threshold number "C1" host pairs, and the an historical number of host pairs is smaller than the threshold number by a first factor value "C2", then
indicating that the new host is a scanner.
2. (Original) The method of claim 1 wherein "C1" and "C2" are adjustable thresholds.
3. (Original) The method of claim 2 wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table.
4. (Currently Amended) The method of claim 3, further comprising:
aggregating records from the current time-slice table into a long second update period table, the second update period table having a period that is greater in duration than the first update period; and
checking for ping scans at the end of a long the second update period; and

indicating hosts which produced more than "C3" new host pairs over the ~~long~~ second update period.

5. (Currently Amended) The method of claim 4 wherein indicating, further comprises:
at the end of the ~~long~~ second update period, accessing the ~~long~~ a second update connection table to determine new host pairs that the process had not previously determined;
determining the number of new host pairs added to the table over the ~~long~~ second update period; and
if a host has made more than a first threshold number "C4" host pairs, and the number of host pairs is smaller than the threshold number by a first factor value "C5", then
indicating the new host as a scanner.

6. (Original) The method of claim 1 further comprising:
maintaining Address Resolution Protocol (ARP) packet statistics in the connection table
and for sparse subnets tracking the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks.

7. (Original) The method of claim 1 wherein the scanning attack is a ping scanning attack.

8. (Previously Presented) A method of detecting port scanning attacks, the method comprises:

retrieving from a connection table logged values of protocols and ports used in host pair connections records in the table;

determining if the number of ports used in an historical profile is smaller by a factor "C1" than a current number of ports being scanned by a host, and if the current number is greater than a lower-bound threshold "C2";

recording that the current number for the host is greater than a lower-bound threshold as an anomaly; and
reporting a port scan.

9. (Original) The method of claim 8 further comprising:
assigning a severity level to the port scan and reporting the severity level of the port scan.

10. (Original) The method of claim 8 wherein the reported severity varies as a function of the deviation from historical norm.

11. (Currently Amended) The method of claim 8 further comprising:
determining from accessing data in the connection table, statistics about TCP reset (RST) packets and ICMP port-unreachable packets, to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the historical profile to increase the severity of a port scan event.

12. (Currently Amended) The method of claim 8 wherein determining occurs at the end of ~~short~~ first duration update periods to detect normal scans.

13. (Original) The method of claim 8 wherein the method includes updating data in the connection table over first durations and determining occurs at the end of long second duration update periods to detect stealthy scans, with the second duration update periods being of a longer duration than the first update periods.

14. (Currently Amended) A computer program product residing on a computer readable medium for detecting scanning attacks, comprises instructions for causing a computer to:
add host-pair connection records to a connection table when ~~each time~~ a host accesses another host;

at the end of a first ~~short~~ update period, accessing the connection table to determine new host pairs;

determine the number of new host pairs added to the table over the first update period;
and

if a host has made more than a first threshold number "C1" host pairs, and the an historical number of host pairs ~~in the profile~~ is smaller than the threshold number by a first factor value "C2", then

indicate to a console that the new host is a scanner.

15. (Original) The computer program product of claim 14 wherein "C1" and "C2" are adjustable thresholds.

16. (Original) The computer program product of claim 14 wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table.

17. (Currently Amended) The computer program product of claim 16, further comprising instructions to:

aggregate records from the current time-slice table into a ~~long~~ second update period table;
check for ping scans at the end of a ~~long~~ the second update period; and
indicate hosts which produced more than "C3" new host pairs over the ~~long~~ second update period.

18. (Currently Amended) The computer program product of claim 17 wherein instructions to indicate, further comprises instructions to:

access the long update connection table at the end of the ~~long~~ second update period;
determine the number of new host pairs added to the table over the ~~long~~ second update period; and

if a host has made more than a first threshold number “C4” host pairs, and an historical the number of host pairs ~~in the profile~~ is smaller than the threshold number by a first factor value “C5”, then

indicate the new host as a scanner.

19. (Original) The computer program product of claim 14 further comprising instructions to:

maintain Address Resolution Protocol (ARP) packet statistics in the connection table; and track the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks.

20. (Previously Presented) A computer program product residing on a computer readable medium for detecting port scanning attacks, the computer program product comprises instructions for causing a processor to:

retrieve from a connection table logged values of protocols and ports used for host pair connections in the table;

determine if the number of ports used in a historical profile is smaller by a factor “C1” than a current number of ports being scanned by a host and the current number is greater than a lower-bound threshold “C2”, to record the anomaly; and

report a port scan to a console.

21. (Original) The computer program product of claim 20 further comprising instructions to:

assign a severity level to the port scan and report the severity level of the port scan.

22. (Original) The computer program product of claim 21 wherein the reported severity varies as a function of the deviation from historical norm.

23. (Original) The computer program product of claim 21 further comprising instructions to:

determine from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event.

24. (Currently Amended) Apparatus comprising:
circuitry for detecting scanning attacks, comprising:
circuitry to add host-pair connection records to a connection table when each time a host accesses another host;
circuitry to access the connection table to determine new host pairs;
circuitry to determine the number of new host pairs added to the table over a short first update period; and
~~if a host has made more than a first threshold number "C1" host pairs, and the number of host pairs in the profile is smaller than the threshold number by a first factor value "C2", then~~
circuitry to indicate to a console that the new host is a scanner when a host has made more than a first threshold number "C1" host pairs, and an historical number of host pairs is smaller than the threshold number by a first factor value "C2".[[.]]

25. (Original) The apparatus of claim 24 wherein "C1" and "C2" are adjustable thresholds.

26. (Original) The apparatus of claim 24 wherein the connection table is a current time-slice connection table and host pair records are added to the current time slice connection table.

27. (Currently Amended) The apparatus of claim 24, further comprising:
circuitry to aggregate records from the current time-slice table into a long second update period table;

circuitry to check for ping scans at the end of a ~~long~~ second update period; and
circuitry to indicate hosts which produced more than "C3" new host pairs over the ~~long~~
second update period.

28. (Currently Amended) Apparatus comprising:
a processing device; and
a computer readable medium tangible embodying a computer program product for
detecting scanning attacks, the computer program product comprising instructions for causing
the processing device to:
add host-pair connection records to a connection table when ~~each-time~~ a host accesses
another host;
at the end of a ~~short~~ first update period, accessing the connection table to determine new
host pairs;
determine the number of new host pairs added to the table over the first update period;
and
if a host has made more than a first threshold number "C1" host pairs, and ~~the~~ an
historical number of host pairs ~~in-the-profile~~ is smaller than the threshold number by a first factor
value "C2", then
indicate to a console that the new host is a scanner.

29. (Original) The apparatus of claim 28 wherein "C1" and "C2" are adjustable
thresholds.

30. (Original) The apparatus of claim 28 wherein the connection table is a current time-
slice connection table and host pair records are added to the current time slice connection table.

31. (Currently Amended) The apparatus of claim 28, wherein the computer program
product further comprises instructions to:

aggregate records from the current time-slice table into a long second update period table;
check for ping scans at the end of a long second update period; and
indicate hosts which produced more than "C3" new host pairs over the long second
update period.

32. (Currently Amended) The apparatus of claim 31 28 further comprises instructions to:
access the long second update connection table at the end of the long second update
period;

determine the number of new host pairs added to the table over the long second update
period; and

if a host has made more than a first threshold number "C4" host pairs, and the an
historical number of host pairs ~~in the profile~~ is smaller than the threshold number by a first factor
value "C5", then

indicate the new host as a scanner.

33. (Previously Presented) Apparatus comprising:

a processing device;

a computer readable medium tangibly embodying a computer program product for
detecting port scanning attacks, the computer program product comprises instructions for causing
a processor to:

retrieve from a connection table logged values of protocols and ports used for host pair
connections in the table;

determine if the number of ports used in a historical profile is smaller by a factor "C1"
than a current number of ports being scanned by a host and the current number is greater than a
lower-bound threshold "C2", to record the anomaly; and

report a port scan to a console.

34. (Original) The apparatus of claim 33 further comprising instructions to:

assign a severity level to the port scan and report the severity level of the port scan.

35. (Previously Presented) The apparatus of claim 34 wherein the reported severity varies as a function of the deviation from a historical norm as determined from the historical profile.

36. (Original) The apparatus of claim 34 further comprising instructions to:
determine from the connection table statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets relative to the profile to increase the severity of a port scan event.